REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 29-08-2015	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 24-Feb-2012 - 23-Feb-2015

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Final Report: Self-Protecting Security for Assured Information Sharing	W911NF-12-1-0081
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 206022

6. AUTHORS	5d. PROJECT NUMBER
Chung-Chu (George) Hsieh	
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Norfolk State University 700 Park Avenue McDemmond Center for Applied Research, Suite 601 Norfolk, VA 23504 -8060	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)	10. SPONSOR/MONITOR'S ACRONYM(S) ARO
U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	11. SPONSOR/MONITOR'S REPORT NUMBER(S) 60475-CS-REP.30

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The main objective of the project is to design and develop the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security critically needed for Assured Information Sharing applications.

The research utilizes a variety of open standards that are commonly used for web services security, e.g., eXensible Access Control Markup Language, XML Encryption, and XML Signature to specify or represent access control

15. SUBJECT TERMS

Information security, XML security, information sharing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Chung-Chu (George) Hsieh
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER 757-823-8313

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Documentation Page		*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2015**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**	
4. TITLE AND SUBTITLE **Self-Protecting Security for Assured Information Sharing**		5a. CONTRACT NUMBER	
		5b. GRANT NUMBER	
		5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)		5d. PROJECT NUMBER	
		5e. TASK NUMBER	
		5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Norfolk State University 700 Park Avenue McDemmond Center for Applied Research, Suite 601 Norfolk, VA 23504 -8060**		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**			
13. SUPPLEMENTARY NOTES **The original document contains color images.**			
14. ABSTRACT **The main objective of the project is to design and develop the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security critically needed for Assured Information Sharing applications.**			
15. SUBJECT TERMS			

14. ABSTRACT
The main objective of the project is to design and develop the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security critically needed for Assured Information Sharing applications.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **46**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Report Title

Final Report: Self-Protecting Security for Assured Information Sharing

ABSTRACT

The main objective of the project is to design and develop the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security critically needed for Assured Information Sharing applications.

The research utilizes a variety of open standards that are commonly used for web services security, e.g., eXensible Access Control Markup Language, XML Encryption, and XML Signature to specify or represent access control policies, results of encryption, and digital signatures, respectively. These standards are extended and used in an integrated manner such that the access control policies, encrypted data, and digital signatures can all be embedded with the digital content that needs to be protected. In addition, these security mechanisms can be applied in a fine-grained manner.

The project has focused on: (a) design and prototype implementation of a new framework for protecting electronic medical records; (b) investigation and design of self-protecting security frameworks for cloud computing and big data environments; and (c) extending the frameworks to support the publish-subscribe architecture.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper
08/09/2014 15.00	ChunSheng Xin, Min Song, Liangping Ma, George Hsieh, Chien-Chung Shen. An Incentivized Cooperative Architecture for Dynamic Spectrum Access Networks, IEEE Trans. Wireless Communication, (10 2013): 5154. doi:
08/22/2013 5.00	Zhengrui Qin, Qun Li, George Hsieh. Defending Against Cooperative Attacks in Cooperative Spectrum Sensing, IEEE Transactions on Wireless Communications, (06 2013): 0. doi: 10.1109/TWC.2013.041913.120516
TOTAL:	**2**

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper
TOTAL:	

Number of Papers published in non peer-reviewed journals:

(c) Presentations

1. C.C. Hsieh, "Big Data and Data Science @ NSU", Tidewater, Big Data Event, December 9, 2014, Newport News, VA.

2. A. Ali and C.C. Hsieh, "Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region", Mathematical Association of America, MD-DC-VA Section, November 7 & 8, 2014, Bowie State University, Bowie, MD.

Number of Presentations: 2.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received   Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received   Paper

08/09/2014   16.00   R. Sye, S. Vincent, W. Hendricks, G. Hsieh. Lessons Learned: Building a Big Data Research and Education Infrastructure,
2014 Intl Conf. on Advances in Big Data Analytics. 21-JUL-14, . : ,

08/22/2013   4.00   Rong-Jaye Chen, George Hsieh. Design for a secure interoperable cloud-based Personal Health Record service,
2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom). 03-DEC-12, Taipei, Taiwan. : ,

08/22/2013   8.00   George Hsieh, Dwijitha Paruchuri, Curtis Steward, Ebelechukwu Nwafor, Deepika Gadam. Lessons Learned: Porting Java Applications to Android,
2013 Intl. Conf. on Software Engineering Research and Practice (SERP'13). 22-JUL-13, . : ,

08/22/2013   9.00   RamaKrishna Mullapudi, George Hsieh. A Monitored Student Testing Application Using Cloud Computing,
2013 Intl. Conf. on Frontiers in Education: Computer Science and Computer Engineering (FECS'13). 22-JUL-13, . : ,

08/22/2013   6.00   George Hsieh, Ebelechukwu Nwafor. A Self-Protecting Security Framework for CDA Documents,
2013 Intl. Conf. on Security and Management (SAM'13). 22-JUL-13, . : ,

08/28/2012   1.00   Reginald Sands, George Hsieh, Wallace Hendricks, Aurelia Williams. Building a Secure Virtual Lab Infrastructure for IT Education,
2012 Int'l Conf. on Frontiers in Education: Computer Science and Computer Engineering (FECS'12). 16-JUL-12, . : ,

08/28/2012   2.00   Rong-Jaye Chen, George Hsieh. Design for a Secure Interoperable Cloud-Based Personal Health Record Service,
IEEE CloudCom 2012 Conference. 03-DEC-12, . : ,

    TOTAL: **7**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received   Paper

    TOTAL:

Number of Manuscripts:

Books

<u>Received</u>   <u>Book</u>

   TOTAL:

<u>Received</u>   <u>Book Chapter</u>

   TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Raymond Sye	1.00	
Venkata Ramya Perumalla	0.64	
Vivek Paul Kanumuri	0.64	
Anuraag Jayaseela Vidyasagar	0.64	
Bruk Befekadu	0.00	
Maurice Lightfoot	0.00	
FTE Equivalent:	**2.92**	
Total Number:	**6**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
C.C. Hsieh	0.71	
FTE Equivalent:	**0.71**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
Darius Jefferson	0.64	Computer Science
Calvin Brown	0.00	Computer Science
Ernest Thomas, III	0.00	Computer Science
FTE Equivalent:	**0.64**	
Total Number:	**3**	

Student Metrics
This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME
Raymond Sye (100%)
Venkata Ramya Perumalla (64%)
Maurice Lightfoot (0%)
Total Number: 3

Names of personnel receiving PHDs

NAME
Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED
Wallace Hendricks	0.00
Linda Winkfield	0.00
FTE Equivalent:	**0.00**
Total Number:	**2**

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Technology Transfer

Part One:

Final Report (for 2/24/2012 – 2/23/2015)

Final Report:
Self-Protecting Security for Assured Information Sharing

Submitted to

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

For

Contract Number: W911NF-12-1-0081
Report Number: 60475-CS-REP
Dates Covered: 02/24/2012 to 02/23/2015

Submitted by

Dr. Chung-Chu (George) Hsieh
Professor, Department of Computer Science
PI, Self-Protecting Security for Assured Information Sharing

August 29, 2015

ABSTRACT

The main objective of the project is to design and develop the integrated, secure, embedded, and fine-grained security frameworks that can be used to provide self-protecting security critically needed for Assured Information Sharing applications.

The research utilizes a variety of open standards that are commonly used for web services security, e.g., eXensible Access Control Markup Language (XACML), XML Encryption (XML-ENC), XML Signature (XML-DSIG) and XML Key Management Specification (XKMS) to specify or represent access control policies, results of encryption, digital signatures, and key management, respectively. These standards are extended and used in an integrated manner such that the access control policies, encrypted data, digital signatures and key management information can all be embedded with the digital content that needs to be protected. In addition, these security mechanisms can be applied in a fine-grained manner.

The project has focused on: (a) design and prototype implementation of a new framework for protecting electronic medical records; (b) investigation and design of self-protecting security frameworks for cloud computing and big data environments; and (c) extending the frameworks to support the publish-subscribe architecture.

1.   INTRODUCTION

This report provides additional information regarding how the research was conducted, as well as the accomplishments of the research and related education activities, for the project entitled "Self-Protecting Security for Assured Information Sharing" that was sponsored by the U.S. Army Research Office for the period of performance from 02/24/2012 to 02/23/2015.

This research and related education activities were all performed at Norfolk State University (NSU) on its main campus in Norfolk, Virginia. The Department of Computer Science (CS) was the unit within which these efforts were carried out.

In this report, the major research activities and achievements will be presented in Section 2. Other related research activities and achievements will be described in Section 3. The student involvement and educational achievements will be discussed in Section 4. Additional major contributions to NSU, Department of Defense (DoD) and other U.S. federal agencies' cybersecurity related research and education initiatives will be reported in Section 5. A summary is provided in Section 6.

2.   MAJOR RESEARCH ACTIVITIES AND ACHIEVEMENTS

For this project, the major research activities and achievements were concentrated in three areas: (a) Self-protecting security for Electronic Medical Records (EMRs); (b) Securing cloud computing environments; and (c) Securing big data environments. They also represented the sequence of extension and expansion of our research in identifying and applying the fundamental

concept of self-protecting security in emerging and more challenging computing paradigms including cloud and big data.

2.1.   Self-Protecting Security for EMRs

To design and develop our domain-specific self-protecting security framework and prototype for electronic medical records, we first chose the Clinical Document Architecture (CDA) as the basis for the resulted document. CDA is an HL7/ANSI Standard for exchanging medical records among service providers in the healthcare industry.

We next designed the CDA-based document architecture to allow XACML, XML-ENC, XML-DSIG and XKMS results and related information be embedded in a CDA document which remains compatible with the CDA standard. In addition, these security mechanisms can be applied in a fine-grained manner such that different sections of the CDA document can be protected with different sets of access control rules, encryption, etc. For instance, the general information for a patient can be viewed by any authorized person including office personnel, nurses, physicians, etc. On the other hand, the diagnostic information can be restricted to the medical personnel only. Figure 1 illustrates the beginning part of a sample CDA document containing the embedded XACML and XML-ENC results and related information.

```
<ClinicalDocument>
 <!-- CDA Header -->
 <StructuredBody>

   <Policy PolicyId = "Policy1">
     <Rule RuleId ="physician">
      <Target>
       <Resource>
        <ResourceContent>
         <EncryptedData>
          <EncryptionMethod/>
          <KeyInfo>
           <KeyName>Key1</KeyName>
          </KeyInfo>
          <CipherData>
           <CipherValue>"Ciphertext1"
           </CipherValue>
          </CipherData>
         </EncryptedData>
        </ResourceContent>
       </Resource>
      </Target>
      <Condition>"PolicyRule1"/Condition>
     </Rule>
   </Policy>
```

Figure 1. Sample Integrated CDA Document

Then we started a series of design and development efforts to implement a prototype software system for the newly designed Self-Protecting Security Framework for CDA for feasibility and demonstration purposes. To facilitate our development effort, we chose to leverage the Model-

Driven Health Tools (MDHT) for CDA[1] which is an open source toolkit developed with significant funding support from the U.S. federal government previously. Figure 2 shows the system architecture for the CDA-based self-protecting security prototype.
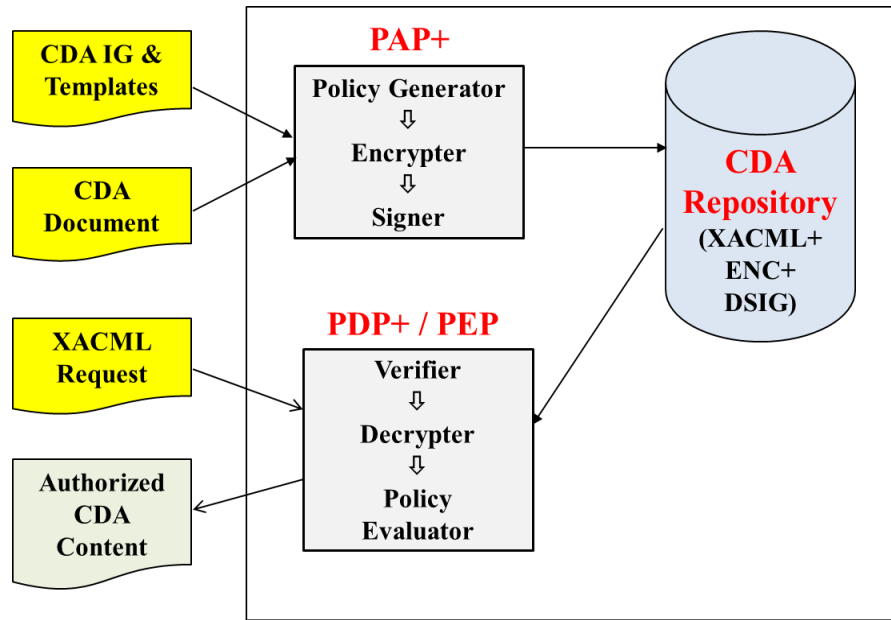

Figure 2. Prototype System Architecture

The design and implementation of the prototype software system was carried out in two stages. The first stage was performed primarily through a M.S. Thesis research entitled *"Generating CDA Documents and Embedding XML Security"* by Deepika Gadam of the CS Department at NSU (Gadam, 2013). It involved the implementation of the capabilities required for generating CDA documents, applying encryption and digital signatures to CDA documents, and validating CDA documents. These capabilities were developed using Java for a Standard Edition Java runtime environment.

The second stage of prototype design and implementation was performed primarily through a M.S. Thesis research entitled *"Prototype Implementation of a Self-Protecting Security Framework for CDA/CCD Documents"* by Ebelechukwu C. Nwafor of the CS Department at NSU (Nwafor, 2013).

The overall research, design and implementation of the CDA-specific self-protecting security framework and prototype system was further published in a peer-reviewed conference paper for the 2013 International Conference on Security and Management (Hsieh & Nwafor, A Self-Protecting Security Framework for CDA Documents, 2013).

In addition, we viewed it important and beneficial to investigate how the CDA-based self-protecting security framework could be leveraged and integrated into the Health Information Network ecosystem. First, we selected the software and source code from CONNECT[2] to

---

[1] http://www.cdatools.org/
[2] http://www.connectopensource.org/

facilitate our prototype development and integration efforts. CONNECT is an open source project designed to enable secure, effective exchange of information. Next, the design and initial prototype implementation efforts were carried out by a M.S. Project entitled "*A Design for Interworking the Self-Protecting Security Framework with CONNECT*" by Lawrence Stroman of the CS Department at NSU (Stroman, 2014).

2.2.   Self-Protecting Security and Cloud Computing

Cloud computing has become a critical technology and paradigm for both public and private sectors, especially federal and state agencies and large to medium enterprises. Cloud computing presents additional security requirements, issues and challenges due to its characteristics in promoting and utilizing virtualization infrastructure, smart and mobile user devices, and resources sharing among multiple tenants.

We viewed that the fundamental concept of self-protecting security could be applied to protect sensitive information in cloud computing and mobile devices environments. Therefore, we viewed this area as a natural extension and expansion of our research on self-protecting security in general.

An important first step in this extension was to investigate how the self-protecting security framework could be effectively applied in a cloud environment especially for Personal Health Records (PHR) which could be controlled and managed by individuals. A PHR is a special form of CDA with the focus of keeping track of long-term personal health information instead of just a single per-episode medical treatment information. This research led to the publication of a peer-reviewed conference paper for the 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (Hsieh & Chen, Design for a Secure Interoperable Cloud-Based Personal Health Record Service, December 2012). Figure 3 illustrates the proposed system design utilizing the self-protecting security framework and advanced cryptographic mechanisms.
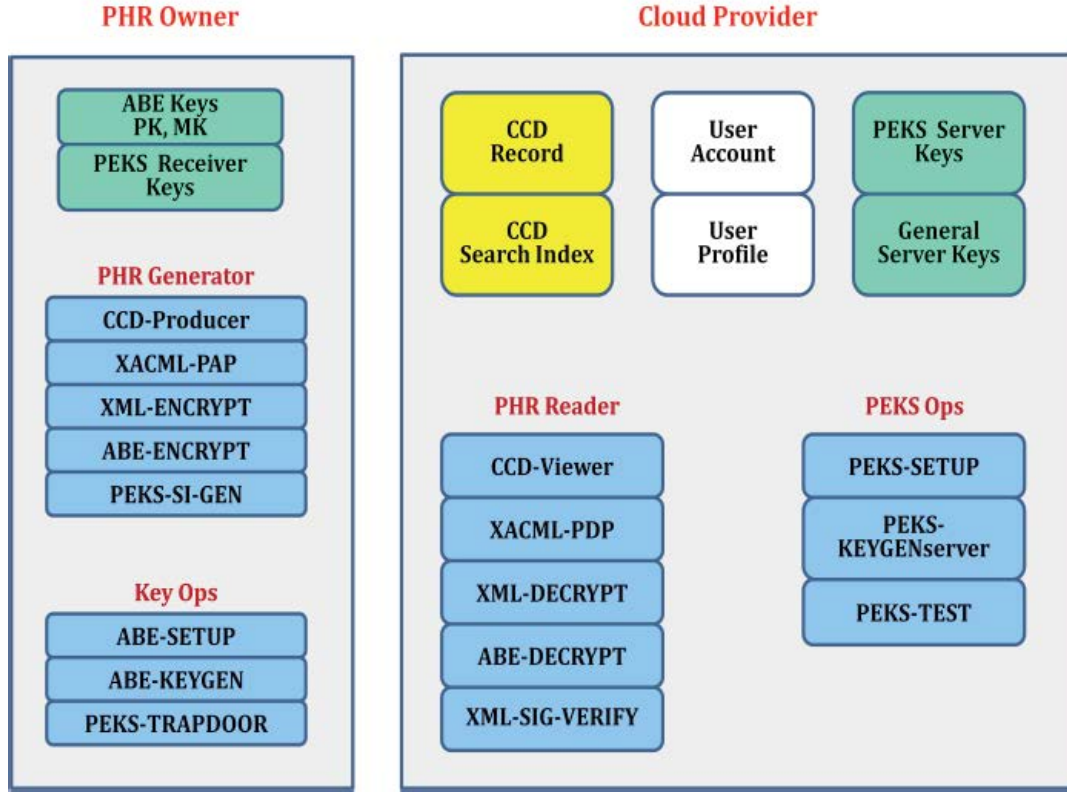
Figure 3. System Architecture for Cloud-Based PHR Service

In addition, we performed several related research and prototype development efforts on cloud and mobile device security and services implementation, in support of the fundamental concept of self-protecting security specifically and privacy/security in general.

1) Porting MDHT to Android. We viewed it a great benefit if the cloud based PHR service could support Android mobile platforms as end user devices for the PHR owners, such that end-to-end security could be enforced while greater convenience could be provided to the users. Thus, we conducted research on the feasibility of porting the MDHT-based self-protecting security capabilities to the Android platform, primarily through a M.S. Thesis entitled "*Developing a Personal Health Record Application for Android Platform*" by Dwijitha Paruchuri of the CS Department at NSU (Paruchuri, 2013). In addition, our research efforts and results were published in a peer-reviewed conference paper entitled "*Lessons Learned: Porting Java Applications to Android*" for the 2013 International Conference on Software Engineering Research and Practice (Hsieh, Paruchuri, Steward, Nwafor, & Gadam, July 2013).

2) Developing Services for Amazon Cloud. Amazon Cloud has been the most popular and powerful public cloud provider since the dawn of cloud computing. We considered it necessary and important to conduct research and experimentation in cloud service development using the Amazon Cloud. This effort was performed primarily through a M.S. Project research entitled *"Monitored Student Testing Service using Cloud Computing"* by RamaKrishna Mullapudi of the CS Department at NSU (Mullapudi R. , 2013). In addition,

6

our research efforts and results were published in a peer-reviewed conference paper entitled *"A Monitored Student Testing Application Using Cloud Computing"* for the 2013 International Conference on Frontiers in Education: Computer Science and Computer Engineering (Mullapudi & Hsieh, July 2013).

3) <u>Building Secure Virtual Lab Environment</u>. We also considered it necessary and important to conduct research, development and experimentation in cloud computing technologies and platforms. We chose to use VMware virtualization infrastructure products to build a secure virtual lab environment for teaching and research at NSU. This effort was performed primarily through a M.S. Project research entitled "*Building Secure Virtual Lab Environments using VMware Virtualization Infrastructure*" by Reginald A. Sands of the CS Department at NSU (Sands R. A., 2011). In addition, our research efforts and results were published in a peer-reviewed conference paper entitled "*Building a Secure Virtual Lab Infrastructure for IT Education*" for the 2012 International Conference on Frontiers in Education: Computer Science and Computer Engineering (Sands, Hsieh, Hendricks, & Williams, July 2012).

4) <u>Android Security</u>. We considered Android security a critical part of the self-protecting security framework especially for mobile and cloud computing. A summer research project focusing on Android security was performed by Daryl A. England and Leah D. Winkfield under the auspices of the 2012 University Research Apprenticeship Program managed by U.S. Army Educational Outreach Program (England & Winkfield, 2012).

5) <u>Developing PHR for Android</u>. Our prior effort in porting MDHT to Android proved that it was too difficult (due to the lack of many Java SE packages on Android platform) and problematic (from performance viewpoint) to complete it successfully. Thus, we investigated an alternative of using Google Health which was a defunct cloud based PHR service provided by Google. The Google Health had software components that ran on Google Cloud and Android smartphones. We investigated the feasibility of leveraging the Android based software components for Google Health for our cloud-based PHR service. This effort was performed primarily through a B.S. Seminar research project entitled "*Developing a Personal Health Record Application for Android*" by Leah D. Winkfield of the CS Department at NSU (Winkfield, 2013).

6) <u>Building Secure Cloud Environments</u>. To facilitate our research, education, and experimentation efforts, we continued to expand the private cloud infrastructures in our lab at NSU by adding more hardware capacity (computing, storage and networking), features and functionalities (fault-tolerance and migration), and VMware vCloud capabilities. These efforts were conducted primarily through three M.S. Projects entitled "*Upgrading the Design and Implementation of a Secure and Scalable Virtual Lab Infrastructure*" (England D. A., 2014), "*Design and Implementation of a vCloud Enabled Secure and Scalable Virtual Lab Infrastructure*" (Evans, 2014), and "*Building a Private Cloud Based Virtual Lab Infrastructure Using VMware vCloud*" (Lightfoot, 2015), respectively.

2.3.   Self-Protecting Security and Big Data

Similarly, big data has become a critical technological ecosystem for both public and private sectors, especially the larger agencies and enterprises. Big data presents additional security requirements, issues and challenges due to its characteristics in distributed computing and storage paradigm.

We viewed that the fundamental concept of self-protecting security could be applied to protect sensitive information in big data environments. Therefore, we viewed this area as a natural extension and expansion of our research on self-protecting security in general. We were especially interested in leveraging Apache Accumulo[3] for cell-based access control.

We started our research in big data with hands-on learning and implementation efforts focusing initially on Apache Hadoop[4] platform capabilities including HDFS, MapReduce and Hive. We installed and configured two types of Hadoop clusters using the two most widely used Hadoop distributions from Hortonworks[5] and Cloudera[6], respectively. These efforts were carried out primarily through a M.S. Project entitled "Managing Hadoop Big Data Environments Using Cloudera and Hortonworks Cluster Management Tools" by Shontae M. Vincent of the CS Department at NSU (Vincent, 2014). In addition, our research efforts and results were published in a peer-reviewed conference paper entitled "*Lessons Learned: Building a Big Data Research and Education Infrastructure*" for the 2014 International Conference on Advances in Big Data Analytics (Hsieh, Sye, Vincent, & Hendricks, 2014).

Next, we conducted research in cybersecurity using big data analytics to identify changes in central nodes based on the real world Internet traffic provided by the Center for Applied Internet Data Analysis (CAIDA)[7] through a M.S. Thesis research entitled "*Network Security Analysis using Big Data Platform*" by Raymond Sye of the CS Department at NSU (Sye, 2013).

Then, we conducted research and implementation in using Accumulo for cell-based access control. These efforts were performed primarily through a M.S. Project research entitled "*Using Accumulo to Provide Access Control for Hadoop-Based Big Data*" by Venkata Ramya Perumalla of the CS Department at NSU (Perumalla, 2014).

In addition, three undergraduate students in the BS.CSC program at NSU conducted research in big data and big data analytics for their capstone Seminar projects entitled "*Big Data and Big Data Analytics*" (Perry, 2014), "*Using Machine Learning Techniques for Network Intrusion Detection*" (Thomas, 2015), and "*Big Data – Log Analysis*" (Brown, 2015), respectively.

3.   OTHER RELATED RESEARCH

Under the general consideration of cybersecurity, we also conducted research in the following areas:

---

[3] http://accumulo.apache.org/

[4] http://hadoop.apache.org/

[5] http://hortonworks.com/

[6] http://www.cloudera.com/content/cloudera/en/home.html

[7] http://www.caida.org/home/

1) <u>Digital forensics</u>. It is necessary and important to use digital forensic techniques to identify vulnerabilities in privacy and security protection. We performed research and experimentation efforts in digital forensics through a M.S Thesis entitled "*DesDROID: Securing Social Networking Applications Metadata on Android Devices*" (Calder, 2014), and a M.S. Project entitled "*Windows Analysis using Open Source Forensics Tools*" (Alatawi, 2014).

2) <u>Smart grid security</u>. We conducted research in using advanced cryptographic schemes proposed for the self-protecting security framework for protecting information sharing on smart grid systems, through a M.S. Project entitled "*Applying Advanced Cryptographic Schemes for Smart Grid Systems*" by John P. O'Sullivan of the CS Department at NSU (O'Sullivan, 2014).

3) <u>Communications security</u>. We were also interested in communications security as a means to assure information sharing. We participated in research that resulted in three peer-reviewed publications: "*Defending against Cooperative Attacks in Cooperative Spectrum Sensing*" (Qin, Li, & Hsieh, 2013), "*An Incentivized Cooperative Architecture for Dynamic Spectrum Access Networks*" (Xin, Song, Ma, Hsieh, & Shen, 2013), and "*Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region*" (Ali & Hsieh, 2014).

4) <u>Extensions of self-protecting security framework</u>. Additional research in extending the self-protecting security framework to support data governance was performed by a MS.CSC student, Rebecca A. Ward, and a research in extending the framework to support the publish-subscribe model was performed by Anthony Nicholas through his M.S. Thesis research (in progress).

4.   RESEARCH-RELATED EDUCATIONAL ACHIEVEMENTS

Through this project, two faculty members at NSU have received research support: Dr. George Hsieh (PI), and Dr. Abdinur Ali (Mathematics Department). In addition, Mr. Wallace Hendricks, IT Manager for the Department of Computer Science and College of Science, Engineering and Technology provided voluntary IT support.

Overall, twenty four undergraduate and graduate students were involved in research directly related to this project and advised by Dr. George Hsieh (PI): Venkata Ramya Perumalla, Vivek Paul Kanumuri, Bruk Befekadu, Raymond Sye, Anuraag Jayaseela Vidyasagar, Maurice Lightfoot, Darius Jefferson, Calvin Brown, Ernest Thomas, John P. O'Sullivan, Lawrence Stroman, Daryl England, Dominique Calder, Hanan Alatawi, Shontae Vincent, Terrell Evans, Kaila Perry, Leah D. Winkfield, Ebelechukwu Nwafor, RamaKrishna Mullapudi, Deepika Gadam, Dwijitha Paruchuri, Anthony Nicholas, and Rebecca Ward.

Nineteen of these 24 students had used these research efforts directly related to this project to complete their degree-required capstone research for M.S. or B.S. degrees.

Ten of these 24 students had received partial stipend support from this project. After graduation, one went on to a PhD in Computer Science program, and two went on M.S. programs (Computer Science and Cybersecurity, respectively).

5.   CONTRIBUTIONS TO RESEARCH & EDUCATION INITIATIVES

This project has been an important part of the research, education and workforce development initiatives at the Department of Computer Science, and the National Center of Academic Excellence in Information Assurance Education (CAE/IAE) at NSU which was designated by the Department of Homeland Security and National Security Agency in 2009. In May 2015 NSU was notified by NSA and DHS that it has been re-designated as a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) through academic year 2020. Again, this project made important contribution to NSU's earning the re-designation.

This project also made very important contribution to the awarding and implementation of another ARO funded project at NSU entitled "*Building a Cloud Computing and Big Data Infrastructure for Cybersecurity Research and Education*" (PI: Dr. George Hsieh, $497,725, 1 Feb 2014 - 31 Jan 2015). The knowledge, experience and expertise achieved through this project were directly leveraged to prepare and then implement the second project.

In addition, these two ARO funded projects made important contributions to the awarding and implementation of a recently launched major initiative entitled "*Consortium for K-20 Cybersecurity Workforce Development*" and funded by the National Nuclear Security Administration ($25M, 1 Oct 2014 - 30 Sep 2019). NSU is the lead of this Consortium consisted of thirteen HBCU/MSI, two DOE national labs, one local school district, and SPAWAR. Dr. George Hsieh serves as a co-PI for NSU responsible for leading research and capacity building efforts for the Consortium.

Furthermore, these two ARO funded projects made significant contributions to the awarding and implementation of a recently launched major initiative entitled "*Center of Excellence in Cyber Security*" and funded by the DoD and managed through the Air Force Research Laboratory (PI: Dr. George Hsieh, $4.98M, 14 Apr 2015 - 14 April 2020). The Center at NSU also includes two academic partners: Old Dominion University (ODU) and Tennessee State University (TSU).

6.   SUMMARY

This project has provided excellent support to the faculty and students at NSU to conduct research, learning, prototype development and experimentation in a variety of critically important subject areas: self-protecting security framework, protecting security and privacy of electronic medical records, cloud computing and security, and big data and security.

Through this three-year project, significant results were achieved in both research and research-related education, including the publication of two journal papers and seven peer-reviewed conference papers. In addition, it provided valuable research experiences and research support to

twenty four undergraduate and graduate students at NSU, with nineteen of these students using the project-related research to complete their degree-required capstone research.

Furthermore, this project has made significant contributions to four major cybersecurity research, education and workforce development initiatives undertaken by DoD, DHS/NSA, DoE/NNSA and NSU. Three of these initiatives will continue until late 2019 or mid 2020 timeframe. Thus, the achievements and impact of this project will continue to be leveraged for several years to come.

In conclusion, we sincerely appreciate this great opportunity and support provided by ARO and the DoD community. We believe that we have successfully executed the program and achieved significant results. We look forward to continuing our close collaboration with the DoD.

REFERENCES

Alatawi, H. S. (2014). *Windows Analysis using Open Source Forensics Tools.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Ali, A., & Hsieh, G. (2014). Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region. *Mathematical Association of America, MD-DC-VA Section.* Bowie, MD.

Brown, C. (2015). *Big Data – Log Analysis.* B.S. Seminar Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Calder, D. (2014). *DesDROID: Securing Social Networking Applications Metadata on Android Devices.* M.S. Thesis, Norfolk State University, Department of Computer Science, Norfolk, VA.

England, D. A. (2014). *Upgrading the Design and Implementation of a Secure and Scalable Virtual Lab Infrastructure.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

England, D. A., & Winkfield, L. D. (2012). *Self-Protecting Security for Assured Information Sharing (Android Security).* Final Research Report for 2012 URAP, Norfolk State University, Department of Computer Science, Norfolk, VA.

Evans, T. S. (2014). *Design and Implementation of a vCloud Enabled Secure and Scalable Virtual Lab Infrastructure.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Gadam, D. (2013). *Generating CDA Documents and Embedding XML Security.* M.S. Thesis, Norfolk State University, Department of Computer Science, Norfolk, VA.

Hsieh, G., & Chen, R.-J. (December 2012). Design for a Secure Interoperable Cloud-Based Personal Health Record Service. *IEEE 4th Int'l Conf. on Cloud Computing Technology and Science (CloudCom'12)*, (pp. 472-479). Taipei, Taiwan.

Hsieh, G., & Nwafor, E. (2013). A Self-Protecting Security Framework for CDA Documents. *Proc. 2013 Intl Conf. on Security and Management (SAM'13)*, (pp. 251-257). Las Vegas, NV.

Hsieh, G., Paruchuri, D., Steward, C., Nwafor, E., & Gadam, D. (July 2013). Lessons Learned: Porting Java Applications to Android. *2013 Int'l Conf. on Software Engineering Research and Practice (SERP'13)*, (pp. 530-536). Las Vegas, NV.

Hsieh, G., Sye, R., Vincent, S., & Hendricks, W. (2014). Lessons Learned: Building a Big Data Research and Education Infrastructure. *Proc. 2014 Intl Conf. on Advances in Big Data Analytics (ABDA'14)*, (pp. 209-215). Las Vegas, NV.

Lightfoot, M. (2015). *Building a Private Cloud Based Virtual Lab Infrastructure Using VMware vCloud.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Mullapudi, R. (2013). *Monitored Student Testing Service using Cloud Computing.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Mullapudi, R., & Hsieh, G. (July 2013). A Monitored Student Testing Application Using Cloud Computing. *2013 Int'l Conf. on Frontiers in Education: Computer Science and Computer Engineering (FECS'13)*, (pp. 433-439). Las Vegas, NV.

Nwafor, E. C. (2013). *Prototype Implementation of a Self-Protecting Security Framework for CDA/CCD Documents.* M.S. Thesis, Norfolk State University, Department of Computer Science, Norfolk, VA.

O'Sullivan, J. P. (2014). *Applying Advanced Cryptographic Schemes for Smart Grid Systems.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Paruchuri, D. (2013). *Developing a Personal Health Record Application for Android Platform.* M.S. Thesis, Norfolk State University, Department of Computer Science, Norfolk, VA.

Perry, K. (2014). *Big Data and Big Data Analytics.* B.S. Seminar Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Perumalla, V. R. (2014). *Using Accumulo to Provide Access Control for Hadoop-Based Big Data.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Qin, Z., Li, Q., & Hsieh, G. (2013, June). Defending Against Cooperative Attacks in Cooperative Spectrum Sensing. *IEEE Transactions on Wireless Communications, 12*(6), 2680-2687.

Sands, R. A. (2011). *Building Secure Virtual Lab Environments using VMware Virtualization Infrastructure.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Sands, R., Hsieh, G., Hendricks, W., & Williams, A. (July 2012). Building a Secure Virtual Lab Infrastructure for IT Education. *2012 Int'l Conf. on Frontiers in Education: Computer Science and Computer Engineering (FECS'12).* Las Vegas, NV.

Stroman, L. (2014). *A Design for Interworking the Self-Protecting Security Framework with CONNECT.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Sye, R. (2013). *Network Security Analysis using Big Data Platform.* M.S. Thesis, Norfolk State University, Department of Computer Science, Norfolk, VA.

Thomas, E. (2015). *Using Machine Learning Techniques for Network Intrusion Detection.* B.S. Seminar Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Vincent, S. M. (2014). *Managing Hadoop Big Data Environments Using Cloudera and Hortonworks Cluster Management Tools.* M.S. Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Winkfield, L. D. (2013). *Developing a Personal Health Record Application for Android.* B.S. Seminar Research Project, Norfolk State University, Department of Computer Science, Norfolk, VA.

Xin, C., Song, M., Ma, L., Hsieh, G., & Shen, C.-C. (2013, Oct). An Incentivized Cooperative Architecture for Dynamic Spectrum Access Networks. *IEEE Transactions on Wireless Communications, 12*(10), 5154-5161.

Part Two:

Attachment for Final Reporting Period

(for 8/1/2014 – 2/23/2015)

REPORT DOCUMENTATION PAGE (SF298)
(Continuation Sheet)

(1) Submissions or publications under ARO sponsorship (from 01-Aug-2014 to 23-Feb-2015):

  (b) Presentations

      i. Presentations at meetings, but not published in Conference Proceedings: 2

          1. C.C. Hsieh, "Big Data and Data Science @ NSU", Tidewater, Big Data Event, December 9, 2014, Newport News, VA.

          2. A. Ali and C.C. Hsieh, "Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region", Mathematical Association of America, MD-DC-VA Section, November 7 & 8, 2014, Bowie State University, Bowie, MD.

Presentations at Meetings

1. C.C. Hsieh, "Big Data and Data Science @ NSU", Tidewater, Big Data Event, December 9, 2014, Newport News, VA.

Big Data and Data Science @ NSU

Dr. George Hsieh

Department of Computer Science
Norfolk State University

December 9, 2014

Overview

- ⌘ A new research initiative launched in summer 2013
- ⌘ Current efforts
  - ⌃ Receiving funding support from three research grants
  - ⌃ Additional funding support from education grants
  - ⌃ Actively engaging students in research projects
  - ⌃ Ramping up expertise and research infrastructure
- ⌘ Exploring new opportunities
  - ⌃ Cybersecurity Research
  - ⌃ Education
  - ⌃ Collaboration

Current Funding Support

⌘ Research grants providing funding support

- **Building a Cloud Computing and Big Data Infrastructure for Cyber Security Research and Education, Army Research Office**, **$497K**, Feb 2014 - Jan 2015, for equipment purchase to implement a research and education infrastructure for cloud computing and big data

- **Self-Protecting Security for Assured Information Sharing, Army Research Office**, **$487K**, Feb 2012 - Feb 2015, for design and development of integrated, secure, embedded, and fine-grained security frameworks to provide self-protecting security

- **Massie Chair of Excellence in Information Assurance and Cyber Security, Department of Energy**, Sep 2009 - Mar 2015, cloud computing security and forensic analysis research subproject

⌘ Education program grants

- Title III (US Department of Education)
- Special Funding (Commonwealth of Virginia)
- NSF and DoD Cybersecurity Scholarship Grants

Research Highlights

⌘ Previously
  - ⌃ Focused on learning & small-scale application development projects
  - ⌃ **Published a refereed conference paper:** "Lessons Learned: Building a Big Data Research and Education Infrastructure", *2014 Intl. Conf. on Big Data Analytics*, July 2014

⌘ Currently
  - ⌃ **4** faculty/staff members on research team
  - ⌃ **3** undergraduate and **8** graduate students doing research
  - ⌃ Investigating a broad array of Hadoop technologies & applications for cybersecurity intelligence
  - ⌃ E.g., **2** graduate students completing degrees this month
    - ⊠ Network Security Analysis using Hadoop Big Data Platform
    - ⊠ Using Accumulo to Provide Access Control for Hadoop-Based Big Data

⌘ Good news: no difficulty in attracting highly qualified & interested students

Research Areas

Category	Subject Area
Application Domains	**Network structure analysis**
	Network data analysis
	Intrusion and anomaly detection
	Event log analysis
	Data analysis and machine learning
Hadoop Tools	**Graph-processing (Giraph)**
	Text search (Solr)
	Log processing (Flume)
	Security - access control (Accumulo)
	Real-time processing (Storm)
	Lightning-fast cluster computing (Spark)
	Database (Mongo)
	Database (Cassandra)
	Database (HBase)
	Machine learning (R-Hadoop)

Research Infrastructure

- ⌘ Established a small-scale lab initially
  - ⌃ Using existing PC's, workstations, and servers
  - ⌃ Installed and configured 3 multi-node Hadoop clusters for learning and research (using both Cloudera and Hortonworks distributions)
- ⌘ Expanding with new equipment
  - ⌃ Hardware equipment vendor: Dell
  - ⌃ A **6-node Hadoop cluster** (integration and testing)
    - ☒ HW/SW installed by students and operational since October
    - ☒ **Cloudera CDH and CM 5.1.2 release**
  - ⌃ A **17-node Hadoop cluster** (production)
    - ☒ HW/SW installation by Dell completed on 5 Dec 2014
    - ☒ **Cloudera CDH and CM 5.2.1 release**
    - ☒ **Cloudera Enterprise – Basic Edition** subscription for one year
    - ☒ Procurement lessons learned: unexpected delay caused by service contracts/SW licenses negotiation/approval (after receiving HW)
  - ⌃ Additional cloud computing equipment being installed
  - ⌃ Adding ~650 Xeon CPU cores, 360 terabytes of hard disk storage, and 3.4 terabytes of RAM

Enhancing Research Infrastructure

System	Function	Server	#Proc	#Core	RAM (GB)	Hard Disk (GB)	Qty
Hadoop-Production	Master Node	R720xd	2	24	128	3,600	5
	Data Node	R720xd	2	24	64	24,576	12
	Subtotal:		**34**	**408**	**1,408**	**312,912**	**17**
Hadoop-Integration	M/D Node	R720xd	2	24	128	3,600	5
	Subtotal:			**120**	**640**	**18,000**	**5**
Cloud-Production	VRTX	M620	2	16	256	30,720	4
	Subtotal:		**8**	**64**	**1,024**	**30,720**	**4**
Cloud-Integration	IBM HS22	7870H5U	2	12	84	4,800	5
	Subtotal:		**10**	**60**	**420**	**4,800**	**5**
	TOTAL:		**62**	**652**	**3,492**	**366,432**	

Exploring Opportunities

- **K-20 Cybersecurity Workforce Pipeline Project**
  - Proposal submitted to **Department of Energy** in July 2014
  - NSU is lead institution for a consortium (PI: Dr. Sandra J. DeLoatch, Provost and VP for Academic Affairs @ NSU)
  - A **research** component included for working with Lawrence Livermore and Sandia National Labs
- **Cyber Analysis, Simulation and Experimentation Environment (CASE-V)**
  - Collaboration with **Old Dominion University/VMASC** (Dr. Jose Padilla) and Tennessee State University (Dr. Sachin Shetty)
  - Include using big data and data analysis to inform M&S operations and analyze M&S results
- **US Army Training Brain Operations Center (TBOC)**
  - Exploring student internship and joint research opportunities (Mr. Tony Cerri, Data Transformation Lead)
- **Education**
  - Courses in big data, cloud computing, data science
  - Graduate certificate programs, degree programs

Summary

- ⌘ NSU has established a solid foundation in big data research and education
- ⌘ NSU plans to actively expand its efforts in big data research and education
- ⌘ NSU is eager to explore collaboration opportunities with government and private sectors on big data and data science

- ⌘ Contact Information:

  Chung-Chu (George) Hsieh, Professor

  Department of Computer Science, Norfolk State University

  (Tel) 757-823-8313, (Email) ghsieh@nsu.edu

Tidewater Big Data Event

December 9, 2014

Agenda

Time	Session
08:00am - 08:25am	**Registration and Breakfast**
08:25am - 08:35am	**Welcome and Opening Remarks** Abe Usher, CTO, HumanGeo Group
08:35am - 08:55am	**The Future of Data Management: The Enterprise Data Hub** Tom Reilly, CEO, Cloudera
08:55am - 09:55am	**The Motivation of Hadoop (Part 1): Hadoop-able Problems** Annette Baldenegro, Instructor, Cloudera University
09:55am - 10:10am	**Networking Break**
10:10am - 11:10am	**The Motivation for Hadoop (Part 2): Common Hadoop Applications, Interesting Use Cases** Annette Baldenegro, Instructor, Cloudera University
11:10am - 11:25am	**Hadoop in 15 Minutes** Webster Mudge, Senior Director of Technology Solutions, Cloudera
11:25am - 11:55am	**The Future of Intelligence Community Sharing** Gus Taveras, CIO, Patrocinium Systems LLC
11:55am - 12:20pm	**The DoDIIS App Engine - The Gateway to iCITE** Steve Touw, Software Engineer, 42Six Solutions, a CSC Company
12:20pm - 01:30pm	**Lunch and Afternoon Keynote** Karen R. Jackson, Secretary of Technology, Commonwealth of Virginia
01:30pm - 02:00pm	**From Data Management to Insight: Empowering the Data Analyst with Insight Cloud** Jim Stokes, VP Insight Technology Solutions, DigitalGlobe
02:00pm - 03:00pm	**First Round - Lightning Talks** Manjula Ambur, Associate CIO for Big Data Analytics and Chief Knowledge Officer, NASA Langley Research Center Ed McLarney, Associate CIO for Innovation & Technology in the Office of the CIO, NASA Langley Research Center Matt Twiggs, VP & Founder of the Engineering Sector, BOSH Global Services, Inc. Dr. George Hsieh, Professor in the Department of Computer Science, Norfolk State University Audie Hittle, CTO Federal, EMC Emerging Technology Division (ETD)
03:00pm - 03:15pm	**Networking Break**
03:15pm - 04:00pm	**Second Round - Lightning Talks** Tony Cerri, Data Transformation Lead, TRADOC G2's Training Brain Operations Center (TBOC) Paul Tamburello, Senior Lead Engineer & Data Scientist, Booz Allen Hamilton Ray Champoux, Senior Knowledge Engineering Architect, Attensity
04:00pm - 04:30pm	**The Importance of a Data Strategy: Your Path to Success** Amy O'Connor, Big Data Evangelist, Cloudera
04:30pm	**Closing Remarks** Al Di Leonardo, CEO, HumanGeo Group

Presentations at Meetings

2. A. Ali and C.C. Hsieh, "Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region", Mathematical Association of America, MD-DC-VA Section, November 7 & 8, 2014, Bowie State University, Bowie, MD.

Mathematical Association of America
MD-DC-VA Section, November 7 & 8, 2014
Bowie State University
Abstracts

Abstracts for the workshop and invited addresses are listed first, in chronological order, followed by faculty abstracts alphabetized by submitting presenter's last name. Graduate student presentation abstracts and undergraduate student presentation abstracts follow (all alphabetized the same way).

Invited Addresses

FRIDAY WORKSHOP
Gwyneth Whieldon, Hood College
Integrating Tablets into the Mathematics Classroom
4:00 PM, Theater, Student Center
Many college students have tablets, phones, and laptops (often all out in front of them in the same class), but those devices often function more as distractions than as learning tools. This doesn't have to be the case: from function visualization tools and electronic textbooks to effective note-taking software and group collaboration apps, there are plenty of ways to integrate mobile devices into the mathematics classroom in ways that avoid distractions, gimmicks, or time-wasting. Similarly, on the faculty side, there are apps that make it easier to create and distribute innovative course materials, or keep track of student involvement, questions and resources. This is hands-on workshop on how to use web or mobile-based apps in the math classroom, with a focus specifically on calculus, precalculus and linear algebra. Participants should bring their own device to the workshop, as only a limited quantity of iPads will be available as extras.

BANQUET ADDRESS
Craig Bauer, York College of Pennsylvania
Unsolved: History's Greatest Ciphers
8:00 PM, Ballroom A, Student Center
While developments in cryptanalysis (the art/science of cracking ciphers) have forced enciphering techniques to become more and more sophisticated, there remain scores of ciphers stretching back to antiquity that remain unsolved. These were created variously by professional cryptographers, amateurs, artists, killers, and victims. In some cases the identity of the author is also unknown. The talk covers many of these mysteries, along with some mathematics that provides a glimmer of hope for those seeking the solutions. These solutions could reveal the identity of a serial killer or spy, provide the exact location of buried treasure worth millions, expose a secret society, illuminate our understanding of ancient history, or even rewrite the history of science.

SATURDAY INVITED ADDRESSES
Valentina Harizanov, The George Washington University
Computable Mathematics
9:45 AM, Theater, Student Center
In 1936, Turing invented the Turing machine and established formal computability theory as a rigorous mathematical theory of algorithms. Computability theory paved the way for the creation of the modern programmable computer. The main thrust of the field is to understand the power and limitations on algorithmic computation without regard for the physical implementation. Interaction of computability theory with algebra, as well as other areas of mathematics, has resulted in computable structure theory and, more generally, computable mathematics, a very active research area in the last few decades. The talk will focus on the history and significance of computability theoretic ideas and methods in mathematics, including undecidability problems, complexity of truth, and the Gödel incompleteness theorem. We will also discuss algorithms with oracle information, Turing degrees, and some of our recent results.

Abstracts

Larry Washington, University of Maryland
Cannonballs, Triangles, and Secrets: An introduction to elliptic curve cryptography
2:05 PM, Theater, Student Center
Elliptic curves have been around for centuries, but recently they have become very important in cryptography. I'll start with a light introduction to elliptic curves and then discuss some recent cryptographic applications.

Contributed Papers by Author (non-student)

Bill Abrams, Longwood University
Teaching Discrete Mathematics to First Year Majors
3:15 PM, Ballroom C, Student Center
The Longwood University Department of Mathematics and Computer Science, as of Fall 2013, requires a Discrete Mathematics course of all majors. This course is meant to be taken during their first year. I will talk about what motivated us to create this course, what the goals of this course were (and what I think they should be), what material was covered and why, the difficulty of using a book that is not entirely accessible to first year majors, and what I learned from teaching the course the first time.

Emmanuel Addo, American University
Ben Muirhead (Graduate Student), American University
Every Vote Counts - Exit Poll Project
9:15 AM, Columbia Room, Student Center
In Fall 2013 an exit poll was conducted in Northern Virginia to explore the effect of voter ID laws on voter turnout, as a pilot project for a more extensive poll this fall in DC, Northern Virginia, and suburban Maryland. A graduate class in survey sampling designed the survey based on stratified sampling by income and racial composition of precincts; undergraduate students in basic statistics classes conducted the exit poll to determine how many potential voters were turned away because of voter ID requirements. The results of the 2013 project are known and will be presented. The results from 2014 will be known after November 4.

Abdinur Ali, Norfolk State University
Chung-Chu (George) Hsieh, Norfolk State University
Analysis of Antenna Coupling and Magnetic Fields within the Near-Field Region
3:40 PM, Ballroom B, Student Center
Near field communication (NFC) devices are designed to work in short ranges. Communications are exchanged between two NFC-enabled devices by touching or by holding devices in close proximity to each other. NFC-enabled devices can detect other devices in close proximity and interact. These devices successfully function when there are tight couplings between readers and tags. The overall aim of this research is to understand the structure of near fields and to develop suitable antennas for near-field communications. This research was supported by the U.S. Army Research Office under grant number W911NF-12-1-0081.

Bud Brown, Virginia Tech
Multipliers of Difference Sets and How to Find Them
11:05 AM, Ballroom B, Student Center
A (v,k,λ) **difference set** is a k-element subset D of $V=\mathbf{Z}$ mod v such that every nonzero element of V can be expressed as a difference a-b of elements $a,\, b \in D$ in exactly λ ways. A *multiplier* of a (v,k,λ) difference set D on $\mathbf{Z}$ mod v is an integer m such that (a) m and v are relatively prime, and (b) the mapping $x \rightarrow mx$ mod v permutes the set $\{D+j \mid 0 \le j \le v\text{-}1\}$ of shifts of D mod v. This talk will be about multipliers of difference sets and how to find them. There will also be some pretty pictures.

Abstracts

James Case, SIAM
Efficient Extraction From An Exhaustible Energy Source
11:05 AM, Columbia Room, Student Center
Previous investigations have asked how to make as much money as possible from a given source of fossil fuel. With supplies now nearing exhaustion, it becomes more important -- to society if not to energy companies -- to harvest the largest possible quantity of energy. The problem has a surprising multiplicity of solutions.

Hongwei Chen, Christopher Newport University
Three Real Variable Proofs of the Euler Reflection Formula
8:50 AM, Annapolis Room, Student Center
Among the many beautiful formulas involving the gamma function, the Euler reflection formula is particularly significant, as it connects the gamma function with the sine function. In this talk, we present three real variable proofs of this formula. For deriving this formula, we use the differential equation and functional equation.

Ray Cheng, Old Dominion University
The Best Mate Search Strategy
8:50 AM, Ballroom B, Student Center
A female searching for a mate might adopt a threshold based strategy, i.e., select the first male that meets or exceeds a threshold T in quality. Or, she could use a "best-of-N" strategy. Under simple hypotheses, including a fixed cost per prospect, each strategy could be optimized. Which approach is superior? What if the female can set both a threshold T and a maximum search length N?

Boyd Coan, Norfolk State University
Old Theorems, Alternate Proofs by Exterior Algebra
3:15 PM, Columbia Room, Student Center
Many are aware of the methods using differential forms to supplement vector analysis, although initially, vector analysis supplanted the Grassmann techniques. For example, at one point in time, Maxwell's equations were reduced to a partial differential equation using vector analysis but it was realized that differential forms may be used as a means of achieving that same goal. Using modern terminology, these alternate techniques have exterior algebra as a foundation. Not only is exterior algebra a valuable tool in analysis, but is of use in other mathematical disciplines as well. In this short note, we give examples of how exterior algebra may be used to prove some old theorems of modern algebra and geometry. "The neglect of the exterior algebra is the mathematical tragedy of our century." ---Gian-Carlo Rota, Indiscrete thoughts (1996)

Randall Cone, Virginia Military Institute
The AMC5 Pilot Event: An MAA MD-DC-VA Section Initiative
8:50 AM, Theater, Student Center
In this session, we discuss the ongoing pilot test for the AMC5 elementary school mathematics initiative. We also discuss strategies for moving beyond the pilot phase to a more established and planned event, perhaps by partnering with AIBL and other organizations. Most importantly, we encourage our MAA DC-DC-VA Section colleagues to engage with us in an open dialogue concerning the philosophy and pedagogical choices made so far in the AMC5's development. For an example of these latter choices, AMC5 now signifies 'The American Mathematics Celebration 5', rather than 'The American Mathematics Competition 5'.

Donna Dietz, American University
Twisty Puzzles for Liberal Arts Math Courses
11:05 AM, Ballroom C, Student Center
The general public tends to presume that anyone who can solve Rubik's Cubes (and similar puzzles) is very smart. Teaching Liberal Arts students how to solve these puzzles is a great way to improve their mathematical self-esteem while teaching them about group theory, modular arithmetic, algorithmic design, 3D geometric visualization and much more. The key realization that makes this possible is that with just 2 or 3 simplistic routines, the pocket cube (or other puzzle) can be solved.   Most published solutions focus on the overall speed of solution rather than reducing human

memorization. By focusing on reducing the number and complexity of the routines, solutions are within reach of all undergrads and can be mastered after just a few class periods. (Students who are good at mathematics tend to learn the pocket cube in well under an hour.)

Ming Fang, Norfolk State University
Issues in Implementing Newton's method
4:05 PM, Ballroom B, Student Center
In this talk, we will discuss several practical issues in implementing Newton's method.

Raymond Fletcher III, Virginia State University
Properties of Self-inversive Cubic Curves
3:15 PM, Annapolis Room, Student Center
Let K be an irreducible cubic curve which inverts onto itself via a circle with center X. A binary operation can be defined on K by setting a*b equal to the third point besides a, b which lies on the line [a,b] and on K. Also a ternary operation f can be defined on K by setting f(a,b,c) equal to the unique fourth point on circle (a,b,c) and on K. We will show that these two operations are related by the formula: f(a,b,c) = X*((X*a)*(b*c)). Using this formula we will show that there exist 2 orthogonal circles, or possibly 3 mutually orthogonal circles which invert K onto itself.

Spencer Hamblen, McDaniel College
Jan Term at the Joint Meetings
4:05 PM, Columbia Room, Student Center
McDaniel College offers a 3-week January Term every winter and offers a number of on-campus and travel courses. In 2011 and 2014 I ran a course centered around bringing students to the Joint Mathematics Meetings. I will discuss some of the difficulties and rewards of structuring an academic and experiential course around a mathematics conference.

Gregory Hartman, Virginia Military Institute
Open Textbooks and APEX Calculus: A Final Report
11:30 AM, Ballroom C, Student Center
In this talk we discuss the growing open textbook movement and reasons why one should be interested in adopting or writing an open-source text. Pleasures and pitfalls of writing one's own text will be discussed, and an overview of open textbook repositories will also be given. We also give a final (well, probably final) report on APEX Calculus, a "Calc 1" through "Calc 3" text that was written under the APEX (Affordable Print and Electronic teXtbook) model and is in use at VMI.

Dan Kalman, American University
Companion Matrices and Difference Equations 2
11:30 AM, Ballroom B, Student Center
A companion matrix is famous in linear algebra as an answer to the problem "Given a monic polynomial p, find a matrix whose characteristic polynomial is p." But companion matrices have several additional interesting properties that deserve to be better known. In particular, there is a strong connection between companion matrices and difference equations. In this talk I will show an explicit reduction to Jordan Canonical Form for a companion matrix whose polynomial has repeated roots, and use it to derive a beautiful matrix equation for the sum of the kth powers of the first n natural numbers.

Caroline Melles, United States Naval Academy
Undergraduate Capstone Projects in Graph Theory and Other Topics
9:15 AM, Ballroom B, Student Center
For the past three years I have run a one-semester capstone course for undergraduate math majors. Students spend the first six weeks reading and lecturing from Graph Theory, A Problem Oriented Approach, by Daniel A. Marcus. The rest of the course is spent on capstone projects. Topics have included: scheduling a volleyball tournament so that no team plays more than two games in a row, applying the Hungarian algorithm to minimize the total travelling distance of the 64

college basketball teams participating in March madness, a study of the graph-theoretic properties of fullerenes, an optimal solution for plebe watch-standing to minimize class time lost, designing a bicycle route for a triathlon, and applying a Markov model to major league baseball data from the 2013 season to calculate scoring indices for various players. Software used includes Gusek, Matlab, Mathematica, Excel, and Sage. I will discuss the course and some of the projects.

Edwin O'Shea, James Madison University
Math for Liberal Arts and the Calculus Pump
4:05 PM, Ballroom C, Student Center
In a liberal arts class that is rigorously reading Euclid, a star student told me "I'm not a math person. I just like proofs." The other star students say more or less the same thing, despite their grappling with Elements at the level and depth of a very good senior math major. The stars have two things in common: they are all female and they were somewhat successful but indifferent to most of their high school math experience. What are we to do when the only pump to more math (as the MAA CUPM recommends for liberal art classes) for these potentially strong majors is a calculus path these stars are skeptical to immediately follow? I don't have a comprehensive answer for this question but hope to persuade you that it is a question worth asking and worth grappling with. Ideas, thoughts, even refutations from the audience are sought and welcome!

James Parson, Hood College
Constructive Arguments in an Introduction to Proofs Class
9:15 AM, Ballroom C, Student Center
Textbooks that introduce students to proof often include many nonconstructive arguments, e.g. proofs of "existence" that do not produce examples. I will give illustrations of such arguments and explain how logicians pinpoint what makes an argument constructive or not, arguing that constructive proofs are more vivid and fit well in introductory courses.

Cherng-tiao Perng, Norfolk State University
Some Observations on Klein Quartic, Groups, and Geometry
8:50 AM, Columbia Room, Student Center
The Erlangen Program published by Felix Klein in 1872 remains an effective way of looking at geometry. In Klein's point of view, the study of geometry is the study of the invariants or symmetry under a suitable transformation group. The purpose of this talk is to share some ideas that arose while I was following a proof in Dolgachev's book on algebraic geometry about the simplicity of the automorphism group of the Klein quartic curve. A theorem of Hurwitz says that the maximum size of automorphism group Aut(Y) for any curve Y of genus g greater or equal to 2 is 84(g-1). It is known that the Klein quartic curve X is of genus 3 and Aut(X) has order 168, the maximum possible size for all curves of genus 3, and that this group is simple. In trying to understand the proof, I found some typos, and ways to bypass the part I did not understand. Without going into Klein's original approach, I found a motivating way to introduce an element of order two in Aut(X), and furthermore with the aid of the computer algebra system SAGE, I constructed an explicit isomorphism between Aut(X) and another group of order 168, namely the symmetry group of the Fano plane, which is related to the study of Cayley numbers, or octonions.

Bob Sachs, George Mason University
Teaching the Fundamental Theorem of Calculus for Better Student Understanding
3:40 PM, Ballroom C, Student Center
Calculus instructors know from experience that students have a hard time passing from the integral on a fixed interval to taking the derivative of the integral with moving endpoint. Researchers have documented this too! I will describe a slight variation on this topic. The key idea is to emphasize the difference quotient (F(b)-F(a))/(b-a) and compare with the corresponding integral average of F'(x).

Abstracts

Hamid Semiyari, James Madison University
An efficient Algorithm for Approximating Solutions of Two-Point Boundary Value Problems and Volterra Integrals
9:15 AM, Theater, Student Center

We demonstrate how the Modified Picard method can be applied to Two Point Boundary Value Problems and Volterra Integral Equations. First we present an algorithm for approximating solutions of two-point boundary value problems and then a theorem that gives conditions under which it is guaranteed to succeed. Then we introduce a new algorithm for the case if the original algorithm failed to converge on a long interval. We split the long interval into subintervals and show the new algorithm gives convergence to the solution. Finally, we repose a Volterra equation using auxiliary variables according to Parker-Sochacki in such a way that the solution can be approximated by the Modified Picard iteration scheme.

Amy Shell-Gellasch, Montgomery College
Ancient Indian Verse and the Powers of 2
3:15 PM, Ballroom B, Student Center

Ancient Indian culture regarded the writing of verse as a high art. In fact, even their mathematics was written in verse. An important component of writing verse was Prosody, determining which and how many syllables are stressed in each line of poetry. Ancient Indian's used an ingenious mathematical algorithm to determine how many syllables could be stressed. Given that they did not have exponential notation, their method is more efficient than straight multiplication.

Roman Sznajder, Bowie State University
On Completely Positive Cones
11:30 AM, Columbia Room, Student Center

For a closed cone C in R^n, the completely positive cone of C is the convex cone K_C in the set of symmetric matrices, generated by uu^T with u in C. Such a cone arises in the conic optimization problems. Motivated by the useful properties of the nonnegative orthant and the positive semidefinite cone, in this talk, we investigate irreducibility, self-duality and homogeneity of the cone K_C.

Zheng Tong, Christopher Newport University
Equilibrants, Semipositive Matrices, Calculation and Scaling
4:05 PM, Annapolis Room, Student Center

For square, semipositive matrices A (Ax > 0 for some x > 0), two (nonnegative) equilibrants e(A) and E(A) are defined. Our primary goal is to develop theory from which each may be calculated. To this end, the collection of semipositive matrices is partitioned into three subclasses for each equilibrant, and a connection to those matrices that are scalable to doubly stochastic matrices is made. In the process a certain matrix/vector equation that is related to scalability of a matrix to one with line sums 1 is derived and discussed.

Sara Tyler, Hawkes Learning
Learning: Anytime, Anywhere
3:40 PM, Columbia Room, Student Center

Courseware Development Engineers at Hawkes Learning have designed an innovative, browser-based platform built specifically with the tablet in mind. Our Expert System offers a distinctive approach to mastery-based learning with instant and specific feedback when students make a mistake, thus improving learning outcomes and reducing anxiety. We understand a large number of students still depend on our unique ability to work without internet access. Hawkes will continue to support this by offering dual platforms to you and your students. Join us to learn more and be entered in a raffle for a $50 Amazon Giftcard!

Jill Tysse, Hood College
Irish Dancing Groups: Some fun activities for an undergraduate-level abstract algebra course
8:50 AM, Ballroom C, Student Center

Irish dance is a traditional form of dance originating in Ireland that today can be found all over the world in its various forms – as a social dance, as competitive dancing, and as entertainment in shows like Riverdance and Lord of the Dance

and at St Patrick's Day parades everywhere. We will examine some fun in-class activities involving Irish dance and the group D_4 of symmetries of a square. In particular, we will use our dance moves to investigate the cosets of D_4 in the symmetric group S_4 on four letters. Put on your dancing shoes and bring your best moves!

Sanju Vaidya, Mercy College
Geetha Surendran, Mercy College
Applications of Graph Theory to Chemistry
3:40 PM, Annapolis Room, Student Center
In the last twenty years, many scientists have developed mathematical models to analyze structures of various chemical compounds. Graph theory has provided many powerful tools to solve problems in many areas of chemistry such as chemical isomer enumeration and Quantitative Structure-Property Relationships (QSPR).We will analyze theorems and properties of various types of graphs and their applications to describe molecular formulas of certain types of chemical compounds. Additionally, we will analyze topological indices of molecular graphs and correlate them with structures and properties of certain chemical compounds.

Graduate Student Abstracts by Author

Jasmine Alston, Virginia State University
Mohammad Tabanjeh, Virginia State University
On The Numerical and Algebraic Techniques for Computing Matrix Determinant
11:05 AM, Ballroom A, Student Center
The computation of the sign of a matrix determinant is a well-known problem. It is the problem of testing whether det(A) > 0, det A = 0, or det(A) < 0 for an n-by-n matrix A. This problem finds its application in computational geometry, such as computation of convex hulls, Voronoi diagrams, and testing whether the line intervals of a given family have nonempty common intersection. In this talk, we review, modify and combine various techniques of numerical linear algebra and rational algebraic computations (with no error) to achieve our main goal of decreasing the bit-precision for computing det A or its sign which enable us to obtain the solution with few arithmetic operations. Such a decrease is necessary for many of the computational geometry applications.

Shantanu Awasthi, Virginia State University
Krishan Agrawal, Virginia State University
Youngjin Lu, Virginia State University
Comparison of Mathematica and Empirical Modelling in Studying the Relationship Between Single Fiber and its Bundle
11:30 AM, Annapolis Room, Student Center
In recent years, the significant research is being conducted to create high performance polymer based composite materials. These composite materials have various applications such as ballistic armors and consumer products. This advancement is taking place because a better understanding of the relationship between single fiber strength and its bundle. In this study, a relationship based on transfer ratio between the strengths of single fiber and its bundle is discussed using empirical and mathematical modeling. This is achieved using a real time data sets. In empirical modelling, Anderson Darling test is used via Mini tab and in mathematical modeling, Wei bull distribution is used as probability distribution function for strength of single fiber while normal distribution is used for its bundle based on classical mathematical theory. It is observed that empirical modeling is better predictor of transfer ratio, however mathematical modelling can be used to predict the strength of the bundle using single fiber strength.

Eugene Evans, Virginia State University
Predictive Modeling using Artificial Neural Networks on Polymer Composite Properties
3:15 PM, Ballroom A, Student Center
In this study artificial neural networks (ANN) are utilized to produce a predictive model to investigate the properties of high-performance polymer fibers. This model generalized the behavior between bundled fibers and their single filament counterparts. Several data points are used from the bundled fibers data to determine the average maximum force applied

to break a single filament fiber. In this study five backpropagtion (training methods) methods are compared to determine which method is most effective by using the Mean Absolute Percentage Error (MAPE) of each. This will allow a further understanding of polymer composite properties and possibly make manufacturing processes less expensive by reducing the number of tests when evaluating single filament characteristics. Prior to the comparison of ANNs, appropriately the optimum number of neurons (training cells) is determined. This ensures an adequate comparison of methods.

Lindsey Santos Koos, Old Dominion University
Description of a Computationally Efficient Boltzmann Equation Discretization Algorithm and its Application to Broad Spectrum Neutral and Ionized Space Radiation
9:15 AM, Ballroom A, Student Center
The Boltzmann integro-differential equation describes the propagation of neutral and charged particles within bulk matter. It is a powerful mathematical tool to simulate and study the effect of mono-energetic laboratory radiation beams and a broad-spectrum space radiation environment on biological and solid state end points (targets). In this talk, starting with the 3-dimensional (3D) time and angular dependent Boltzmann transport equation, steps will be discussed to create a computationally efficient 1-dimensional (1D) time and angular independent Boltzmann particle transport equation. Appropriate coordinate transformations will be shown which map the 1D integro-differential equation into a form that allows inversion and discretization. The discretization steps produce three distinct sets of solution methodology for neutral, light particles, and heavy ions. While the bulk of the talk will focus on the mathematical details of the discretization procedure, limited application results will also be shown. For application, the discretized 1D algorithm is applied to the broad energy spectrum of space radiation environment. Here, using the discretized solution, the radiation composition of the free space galactic cosmic rays (GCR) composed of all particles in the periodic table and trapped protons within the Earth geomagnetic field are transported through typical spacecraft material and dosemetric quantities of interest at specific target points are computed. Upon the completion of the particle transport, the computed particle flux quantities are applied to a realistic space vehicle and human phantom models to assess astronaut exposure due to ionizing radiation.

Harry Lang, Johns Hopkins University
A New Proof of the Lovasz Local Lemma
8:50 AM, Ballroom A, Student Center
Traditional proofs of the Lovasz Local Lemma (LLL) rely on the probabilistic method. In 2009, Moser and Tardos presented the first constructive proof, and a series of subsequent papers improved upon their result. In this talk, I will provide a simple proof of the LLL which follows the general idea of recent papers but avoids invoking results from information theory or Kolmogorov complexity.

Dustin J. Robinson, Virginia State University
Self-inversive Group Circle Systems
11:30 AM, Ballroom A, Student Center
Let G be an abelian group and let g be an element of G. Let f be a mapping from G into the projective plane. If for each 4 element subset {a,b,c,d} of G, the corresponding points {f(a), f(b), f(c), f(d)} are cocyclic, then we call the set of points f(G) and the associated circles a (G,g) circle system. We will illustrate several group circle systems and show that some of these invert onto themselves via 2 orthogonal or even 3 mutually orthogonal circles.

John Ross, Johns Hopkins University
Blowing Bubbles in Gaussian Space
3:40 PM, Ballroom A, Student Center
Soap bubbles and soap films are created in nature by minimizing the surface area of the bubble, while keeping the volume of the bubble unchanged. In doing so, soap bubbles of any shape or size will quickly collapse to a stable, spherical shape. In this talk we discuss the mathematics behind this, generalizing the first and second derivative tests from Calculus. We then turn our attention to Gaussian space, and discuss our main result which states that (stable) bubbles will take the form of planes.

Andrew Wills, Virginia Tech
A Glimpse at Bijective Combinatorics
4:05 PM, Ballroom A, Student Center
We will explore some topics in bijective combinatorics by using sets of seemingly innocuous, perhaps even made up, objects to solve difficult algebra problems, without doing the algebra. In particular, we will find combinatorial models for Hall-Littlewood polynomials, a class of symmetric polynomials where different variables are interchangeable. In this case, combinatorial proofs can be simple and elegant, and often give insight into the basic structure of the polynomials.

Undergraduate Student Abstracts by Author

Sophia Novitzky (Senior), Virginia Tech
Mahalia Sapp (Senior), Virginia Tech
Performance Sensitivity in Vertical Geothermal Energy Harvesting Systems
9:15 AM, Annapolis Room, Student Center
Residential geothermal energy systems have the potential to provide a cost-effective, low carbon footprint technology for heating and cooling. The systems use the soil beneath a residence to store thermal energy in the summer and harness energy in the winter. The soil exchanges heat with the coolant that flows through a pipe inserted into a vertical bore. The energy transfer in the soil changes the coolant temperature, setting the efficiency of the residential heating/cooling system. We are interested in finding how the cross-sectional arrangement of pipes in the bore affects the temperature of the coolant as a function of depth. For a given cross-section, we describe the temperature functions of the coolant and the surrounding soil through a system of time-dependent partial differential equations. From these equations, we find a Sturm-Liouville eigenvalue problem in each cross-sectional variable, whose eigenvalue determines the decay rate of the eigenfunction over depth. We find a numerical solution via the finite element method for the eigenpair corresponding to the lowest decay rate. Our results can be used to determine the borehole depth necessary to meet the energy needs of a residence given a desired geometry of the system.

Katie Sipes (Junior), James Madison University
Salt Flux Concentration in the Kidneys
11:05 AM, Annapolis Room, Student Center
The kidneys are an organ in the body that filters the components of the blood plasma. Ions, sugars and salts are the main components filtered out by the glomerulus. Salt is a component that the body has a more challenging time to make the correct concentration to remain in allostasis. The kidneys can either produce a small quantity of very concentrated urine or a large amount of very dilute urine. This process can be modeled mathematically to understand the semipermeability of the kidneys.